

eZ-Audit
Use-Case Specification 1: Manage Users

Version 1.0

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

Revision History

Date	Version	Description	Author
07/17/2002	1.0	Final version created for 7/17 Deliverable Submission	Cody Winter
08/05/2002	1.1	Revised version created for deliverable re-submission	Matt Portolese

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

Table of Contents

1.	Manage Users	4
1.1	Brief Description	4
2.	Flow of Events	4
2.1	Basic Flow	4
2.2	Alternative Flows	5
2.2.1	No Search Capability for Institution and Case Team Administrators	5
2.2.2	Add User	5
2.2.3	Search does not return any results	7
2.2.4	Delete User	7
2.2.5	Desired Search Results not Returned for ED Administrator	7
2.2.6	Profile Information Incorrect or Incomplete	7
3.	Special Requirements	8
3.1	Maintain History of Administrator Changes	8
4.	Preconditions	8
4.1	ED Administrator created manually	8
4.2	Case Team Administrator created	8
4.3	Institutional Administrator created	8
5.	Postconditions	8
5.1	New User must Change Password	8
6.	Extension Points	8
6.1	Requirements in this Use Case	8

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

Use-Case Specification 1: Manage Users

1. Manage Users

1.1 Brief Description

An administrative user will have the ability to create, change, and delete users from the eZ-Audit system. There are three types of administrative users. One is an ED administrator that can manage all users of the system. The institution administrator may manage users for a particular institution of which that administrator is affiliated. The Case Team administrator may manage users for their own case team.

2. Flow of Events

2.1 Basic Flow

The Basic Flow covers an ED Administrator searching for, and changing profile information for a user.

1) Administrator actor selects the option to “manage users”.

The system verifies the privileges of the logged-in user. If the user is not identified as an administrative user, they will not be presented with the option to manage users.

2) System presents the “manage users” search page.

The options presented to the Administrator actor are to search for a user and add a new user. The Administrator actor may search for a user by the following criteria:

- First Name
- Last Name
- Username
- Institution

3) The Administrator actor enters search criteria and performs the search.

The Administrator actor may enter text in as few as one, but up to all four of the search fields. The text entered may be a partial value.

4) The System returns the list of users.

The system will search the user profile database and return a list of users that match the search criteria entered in Step 3. The system displays the following information for each user:

- Last Name, First Name
- Username
- Institution

In addition to the information above, a “delete” option is available for each user. The screen will display a list of 25 users at a time. If the list goes beyond 25, there will be a “paging” option to view the additional results.

5) The Administrator actor selects a user.

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

Both the name of the user and the username may be selected. They are both a link to the profile page for the selected user. The institution name is also a link. If the institution is selected, the list of all the users for that particular institution is displayed.

6) System presents the Administrator actor with the user profile page.

The user profile page contains all of the user profile information stored for the user selected in Step 5. This list of information includes:

- First Name*
- Last Name*
- Institution (if institutional administrator, this field is pre-populated and may not be edited)*
- Case Team (if Case Team administrator, this field is pre-populated and may not be edited)*
- Email address
- Phone Number*
- Extension (optional)
- Fax (optional)
- Username*
- Password*
- Role*

There is an asterisk denoting the fields that are mandatory.

7) Administrator actor modifies user profile information.

The Administrator actor has the ability to modify all fields except those noted on the profile page. All mandatory fields (those identified by the asterisk) must have a valid value entered (subject to field checks).

8) Administrator actor saves modified profile information.

After the “save” command, the system performs client-side checks of each profile field. If the user password has been changed by the Administrator actor, a flag is set which will later require the modified user to change their password as soon as they login to the system.

9) System saves profile information to the user profile database.

If the client-side checks are successful, the profile information is saved to the user profile database.

2.2 Alternative Flows

2.2.1 No Search Capability for Institution and Case Team Administrators

The Institution and Case Team Administrators only manage a limited number of users. Therefore, these users do not necessitate the use of a search. When one of these users selects “Manage Users” as in Step 1 of the Basic Flow, the system automatically presents the list of users for which that user is responsible as in Step 4. For the Institution Administrator, this includes all system users associated with that institution. For the Case Team Administrator, this includes all users on that Case Team.

2.2.2 Add User

After selecting the option to “Manage Users” in Step 1, the Administrator Actor will have the option to use the “Add User” function.

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

1) Administrator Actor selects “Add User”.

2) System presents a blank “Add User” profile page to the Administrator Actor.

The user profile page is presented to the Administrator Actor with all blank fields. This page is a limited set of the fields presented to the user in Step 6. Not all profile information must be entered by the administrator when creating a user. The fields required are:

- First Name
- Last Name
- Username
- Password
- Role
- OPEID (in the case of a new Institutional user)
- Case Team (in the case of a new Case Team user)

3) Administrator actor enters profile information.

A value for each field presented must be entered in order to create a new user. Also, the Administrator actor must select from a list of roles for the new user. The list is as follows:

- ED Admin
- Institution Admin
- Case Team Admin
- Data Entry
- Screener
- Audit Specialist
- Financial Specialist
- Case Assignment
- Case Approval

If the Administrator actor is a Case Team Administrator adding a new user, the list of available roles are:

- Case Team Admin
- Screener
- Audit Specialist
- Financial Specialist
- Case Assignment
- Case Approval

If any of the Case Team roles are selected, the Administrator Actor must enter the Case Team for which the new user is being created.

If the Administrator actor is an Institution Administrator, the only roles that can be assigned are:

- Institution Administrator
- Data Entry

4) Administrator actor saves modified profile information.

After the “save” command, the system performs client-side checks of each profile field. The system will

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

verify that either an OPEID has been entered OR the Case Team. Both of these may not be entered. Also, the system will verify that if an OPEID is entered, only roles associated with an Institutional user may be selected. Similarly, if the Case Team name is entered, only roles associated with a Case Team user may be selected

5) System saves profile information to the user profile database.

If the client-side checks are successful, the profile information is saved to the user profile database. At this time, a flag is set which will require the newly created user to change their password upon their first login to the system.

2.2.3 Search does not return any results

In steps 3 and 4 of the Basic Flow, if the search performed by the ED Administrator does not return any results, the search page will again be displayed with a notification that the search did not return and results and they may try again.

2.2.4 Delete User

As the search results are presented in step 4, a delete button is available for each user returned in the search.

1) Administrator actor selects “delete” button.

Any of the delete buttons displayed by the list of users may be selected.

2) System displays a confirmation message to the Administrator actor.

The system displays a message to the user displaying the First Name, Last Name, and Username of the user selected to delete and asks the Administrator actor to confirm this is the action they desire to perform.

3) Administrator Actor confirms deletion of user.

The Administrator actor confirms deletion. If the deletion is not confirmed, the original list of user is presented unaltered.

4) System displays the new list of users returned by the original search.

The system displays the list of users returned by the original search minus the user deleted in Step 3 of this alternate flow.

2.2.5 Desired Search Results not Returned for ED Administrator

In step 4 of the Basic Flow, when a list of users is returned by a search, the search fields remain at the top of the page populated by the search criteria originally entered. If the Administrator Actor is not presented with the user or users desired, another search may immediately be performed.

2.2.6 Profile Information Incorrect or Incomplete

If the checks performed in Step 8 reveal an incorrect or incomplete entry, the system will return the same profile page marking the fields that are incorrect or incomplete.

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

3. Special Requirements

3.1 Maintain History of Administrator Changes

There is a requirement to maintain a history of all administrator changes. The easiest way to accomplish this will be to create a new row of data in the database every time new user information is saved. The new row will be flagged as valid and the old entry will be invalid. No rows will be deleted.

4. Preconditions

4.1 ED Administrator created manually

The first ED Administrator must be set up in the system manually before this user is able to create any other users as described in this use case. There is no limit to the number of possible ED Administrators created.

4.2 Case Team Administrator created

For the Case Team Administrator to perform any activities described in this use case, the Administrator must be created by either an ED Administrator, or another Case Team Administrator on that same Case Team. There is no limit on the number of Case Team Administrator's.

4.3 Institutional Administrator created

For the Institutional Administrator to perform any activities described in this use case, the Administrator must be created by either an ED Administrator, or another Institutional Administrator associated with the same institution. There is no limit on the number of Case Team Administrator's.

5. Postconditions

5.1 New User must Change Password

During the process of creating a new user as described in this use case, a flag is set noting that the user has a default password. When the new user logs in for the first time, they are required to change the password before performing any other actions in the system.

There will be a manual process to notify the new user of the username and password for the new account. This manual process is TBD.

6. Extension Points

6.1 Requirements in this Use Case

GEN18 The system will support syntax rules that allow the following elements to be incorporated into passwords:· Alphanumeric values· Alpha-only values· Numeric-only values

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

GEN21 The system will support a minimum password length of 8 characters.

GEN22 The system will support syntax rules that enforce at least three of the following conditions on every password:· Uppercase alphabetic characters (A-Z)· Lowercase alphabetic characters (a-z)· Numeral values (0-9)· Non-alphabetic and non-numeric characters (< ! @ # etc.)

GEN24 The system will store passwords in an encrypted state in the credential repository.

GEN29 The System will determine the Institution users access rights based on their role as defined by the Institution Administrator.

GEN38 The System will determine the ED User's access rights based on their role as defined by the ED User Administrator.

GEN62 The system will maintain a history of all Administrator changes.

GEN64 The system will provide capabilities to administer:· Passwords· User names· User data

GEN72 The system will have the ability to allow administrators to reset passwords to the initial login password for the accounts authorized to the administrator.

GEN77 The system will store a user's first name.

GEN78 The system will store a user's last name.

GEN79 The system will store a user's ID.

GEN80 The system will display a user's first name.

GEN81 The system will display a user's last name.

GEN82 The system will display a user's ID.

GEN83 The system will provide a mechanism for an ED User administrator to add ED Users to the System.

GEN85 The system will provide a mechanism for an ED User administrator to change ED User roles in the system.

GEN86 The system will allow the ED User administrator to modify access rights for all user roles.

GEN87 The system will allow ED Administrator to view access rights and privileges of all system users.

GEN88 The system will provide a mechanism for an Institution User administrator to add Institution Users to the System.

GEN90 The system will provide a mechanism for an Institution User administrator to change Institution User roles in the system.

GEN31 The System will support the administration of "write/create" access rights for Institution Users to their own institution data.

GEN39 The System will support the administration of "read" access rights for ED Users.

GEN40 The System will support the administration of "write/create" access rights for ED Users.

GEN41 The System will support the administration of "submit" access rights for ED Users.

GEN42 The System will provide view access rights to the appropriate ED Users (Screener and Case Team Members) for compliance audits.

GEN43 The System will provide update access rights to the appropriate ED Users (Screener and Case Team Members) for compliance audits.

GEN44 The System will provide view access rights to the appropriate ED Users (Screener and Case Team Members) for financial statements.

eZ-Audit	Version: 1.1
Use-Case Specification 1: Manage Users	Date: 08/05/2002
Use Case 1	

GEN45 The System will provide update access rights to the appropriate ED Users (Screener and Case Team Members) for financial statements.

GEN92 The system will display a text message regarding debarred users on the Institution User Management Page.

GEN99 The system will prepopulate Team and Position for the each Ed user on the Admin Profile page.